FILE 'USPAT' ENTERED AT 11:03:31 ON 04 MAR 97

```
  * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
  *              W E L C O M E   T O   T H E                    *
  *         U. S.   P A T E N T   T E X T   F I L E             *
  * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
=> s relational database
          2035 RELATIONAL
          8543 DATABASE
L1         551 RELATIONAL DATABASE
                (RELATIONAL(W)DATABASE)
=> s l1 and fingerprint
          2106 FINGERPRINT
L2           2 L1 AND FINGERPRINT
=> d 1-
```

1. 5,535,322, Jul. 9, 1996, Data processing system with improved work flow system and method; Matthew S. Hecht, 395/201 [IMAGE AVAILABLE]

2. 5,306,049, Apr. 26, 1994, Sports memorabilia authentication kit; John W. Schireck, 283/74; 206/232, 579; 283/56 [IMAGE AVAILABLE]

```
=> s l1 and signature
          8090 SIGNATURE
L3          30 L1 AND SIGNATURE
=> d 1-
```

1. 5,608,904, Mar. 4, 1997, Method and apparatus for processing and optimizing queries having joins between structured data and text data; Surajit Chaudhuri, et al., 395/602; 364/DIG.1 [IMAGE AVAILABLE]

2. 5,602,999, Feb. 11, 1997, Memory system having a plurality of memories, a plurality of detector circuits, and a delay circuit; Gilbert P. Hyatt, 395/401 [IMAGE AVAILABLE]

3. 5,600,726, Feb. 4, 1997, Method for creating specific purpose rule-based n-bit virtual machines; Joseph M. Morgan, et al., 380/49, 4, 25 [IMAGE AVAILABLE]

4. 5,572,733, Nov. 5, 1996, Data processing system which executes composite objects by combining existing objects; Tadamitsu Ryu, et al., 395/701; 364/280, DIG.1 [IMAGE AVAILABLE]

5. 5,566,349, Oct. 15, 1996, Complementary concurrent cooperative multi-processing multi-tasking processing system using shared memories with a minimum of four complementary processors; Ray C. Trout, 395/840; 364/243, 245.5, 245.6, 245.7, 245.9, DIG.1; 395/475, 800, 827, 841 [IMAGE AVAILABLE]

6. 5,563,999, Oct. 8, 1996, Forms automation system; Mary J. Yaksich, et al., 395/768 [IMAGE AVAILABLE]

7. 5,563,998, Oct. 8, 1996, Forms automation system implementation; Mary J. Yaksich, et al., 395/768 [IMAGE AVAILABLE]

8. 5,551,428, Sep. 3, 1996, Automatic routing to selected destinations of storage phosphor images; Wayne W. Godlewski, et al., 128/653.1 [IMAGE AVAILABLE]

9. 5,551,027, Aug. 27, 1996, Multi-tiered indexing method for partitioned data; David M. Choy, et al., 395/617; 364/246.3, 246.8, 247.5, 255.2, DIG.1; 395/416, 421.06, 456, 480, 497.04 [IMAGE AVAILABLE]

10. 5,548,753, Aug. 20, 1996, Automatic electronic mail notification of database events; Steven A. Linstead, et al., 395/601 [IMAGE AVAILABLE]

Pulled

11. 5,542,078, Jul. 30, 1996, Object oriented data store integration environment for integration of object oriented databases and non-object oriented data facilities; Paul A. Martel, et al., 395/612, 614 [IMAGE AVAILABLE]

12. 5,535,322, Jul. 9, 1996, Data processing system with improved work flow system and method; Matthew S. Hecht, 395/201 [IMAGE AVAILABLE]

13. 5,526,506, Jun. 11, 1996, Computer system having an improved memory architecture; Gilbert P. Hyatt, 395/438; 364/243, 245.5, 249, 249.1, 249.2, 249.7, 251, 252, 952, 967, DIG.1, DIG.2 [IMAGE AVAILABLE]

14. 5,459,846, Oct. 17, 1995, Computer architecture system having an imporved memory; Gilbert P. Hyatt, 395/421.04; 364/DIG.1, DIG.2; 395/494 [IMAGE AVAILABLE]

15. 5,438,508, Aug. 1, 1995, License document interchange format for license management system; Robert M. Wyman, 395/208; 380/4; 395/226 [IMAGE AVAILABLE]

16. 5,414,626, May 9, 1995, Apparatus and method for capturing, storing, retrieving, and displaying the identification and location of motor vehicle emission control systems; Rodney T. Boorse, et al., 364/424.037, 424.038; 395/135, 604, 610, 615 [IMAGE AVAILABLE]

17. 5,412,774, May 2, 1995, Apparatus for and method of displaying a data item of a database using the display function of a selected data item; Rakesh Agrawal, et al., 395/340, 346, 357, 604, 978 [IMAGE AVAILABLE]

18. 5,386,571, Jan. 31, 1995, Computer system and method for storing and displaying of a semantically structured entity relationship diagram; Wolfgang Kurz, 395/611; 364/237.3, 286.3, DIG.1; 395/117 [IMAGE AVAILABLE]

19. 5,344,132, Sep. 6, 1994, Image based document processing and information management system and apparatus; Thomas Q. LeBrun, et al., 271/35, 10.08, 18, 110, 111, 122, 256 [IMAGE AVAILABLE]

20. 5,343,527, Aug. 30, 1994, Hybrid encryption method and system for protecting reusable software components; James W. Moore, 380/4, 25, 30 [IMAGE AVAILABLE]

21. 5,319,543, Jun. 7, 1994, Workflow server for medical records imaging and tracking system; Richard K. Wilhelm, 395/203; 364/413.02; 395/208 [IMAGE AVAILABLE]

Pulled 22. 5,306,049, Apr. 26, 1994, Sports memorabilia authentication kit; John W. Schireck, 283/74; 206/232, 579; 283/56 [IMAGE AVAILABLE]

23. 5,270,530, Dec. 14, 1993, Digital radiographic image quality control workstation operable in manual or pass-through modes; Wayne W. Godlewski, et al., 250/208.1, 580, 587 [IMAGE AVAILABLE]

Pulled 24. 5,260,999, Nov. 9, 1993, Filters in license management system; Robert M. Wyman, 380/4 [IMAGE AVAILABLE]

Pulled 25. 5,204,897, Apr. 20, 1993, Management interface for license management system; Robert M. Wyman, 380/4, 25 [IMAGE AVAILABLE]

Pulled 26. 5,191,525, Mar. 2, 1993, System and method for extraction of data from documents for subsequent processing; Thomas Q. LeBrun, et al., 395/761, 792 [IMAGE AVAILABLE]

Pulled 27. 5,182,770, Jan. 26, 1993, System and apparatus for protecting computer software; Geza Medveczky, et al., 380/4; 340/825.34; 380/25, 49 [IMAGE AVAILABLE]

Pulled 28. 5,181,162, Jan. 19, 1993, Document management and production system; Robert M. Smith, et al., 395/792, 615, 779 [IMAGE AVAILABLE]

29. 5,105,365, Apr. 14, 1992, Environmental compliance system; Timothy E. McDaniel, et al., 364/496, 550 [IMAGE AVAILABLE]

30. 4,954,951, Sep. 4, 1990, System and method for increasing memory performance; Gilbert P. Hyatt, 395/421.08; 364/232.8, 237.2, 237.5, 244, 244.3, 245, 245.2, 245.3, 246.91, 247, 247.2, 247.8, 249, 249.1, 249.2,

252, 259, 259.4, DIG.1; 395/800; 968/900, DIG.1 [IMAGE AVAILABLE]
=

```
 * * * * * * RECONNECTED TO U.S. Patent & Trademark Office * * * * * *
SESSION RESUMED IN FILE 'USPAT' AT 11:14:48 ON 04 MAR 97
FILE 'USPAT' ENTERED AT 11:14:48 ON 04 MAR 97
CHARGED TO COST=OFF


=> d his

     (FILE 'USPAT' ENTERED AT 11:03:31 ON 04 MAR 97)

L1           551 S RELATIONAL DATABASE
L2             2 S L1 AND FINGERPRINT
L3            30 S L1 AND SIGNATURE
L4             0 S L1 AND RETINAL SCANNER
L5            68 S L1 AND VOICE
                 SET PAGE SCROLL

=>
```

Primary Reference

Piosenka et al.

```
=> s 4,993,068/pn
L1             1 4,993,068/PN
                 (4993068/PN)
=> s l1 and remote
        198420 REMOTE
L2             1 L1 AND REMOTE
=> d kwic
US PAT NO:      **4,993,068** [IMAGE AVAILABLE]          L2: 1 of 1
```

ABSTRACT:
An unforgeable personal identification system for identifying users at **remote** access control sites. The unforgeable personal identification system generates one-way encrypted versions of physically immutable identification credentials (facial photo, retinal scan, voice and finger prints). These credentials are stored on a portable memory device (credit card size). At a **remote** access control site, the user presents his portable memory device and the encrypted identification credentials are read. The user then submits physically to inputting of his physical identification characteristics to the **remote** access control site. Comparison is performed with the credentials obtained from the memory device and with the user's physical identity to determine whether to allow or deny access at the **remote** site.

SUMMARY:

BSUM(2)

The . . . more particularly to a system for the generation of unforgeable identification credentials and use of these unforgeable identification credentials at **remote** localized sites.

SUMMARY:

BSUM(5)

Still . . . also provides for some form of comparison of the prestored traits with those obtained through the access control devices. A **remote** access control point transmits the data representing the physical trait which it has gathered through one of the above mechanisms to the central repository. The central repository then matches the data obtained from the **remote** access control point with the prestored data retrieved from the data base. If a successful comparison is obtained, the central. . . requested access. Otherwise, the access is denied. Further, these systems may add encryption and decryption of the messages between the **remote** access control point and the central data base repository for security.

SUMMARY:

BSUM(8)

In . . . physical trait identities and a centralized data base, these systems must maintain an online data base for communication with the **remote** access control points. Maintaining an on-line large data base and communication with **remote** sites for each access is very expensive, and poses intolerable access delays during periods of peak transactions. Also, they result. . .

SUMMARY:

BSUM(10)

Accordingly, . . . of the present invention to provide a universally accepted personal identification system providing for low cost identification of personnel at **remote** access control points without the need of a large, on-line centralized data base to control each of the **remote** access control points. In addition to providing the personal identification, the invention also provides a means for conveying unforgeable privilege. . .

SUMMARY:

BSUM(13)

An unforgeable personal identification system positively identifies users at a **remote** access control site. The identification system includes apparatus for generating encrypted physically immutable identification credentials of a user. These credentials. . .

SUMMARY:

BSUM(14)

The **remote** access control site reads the encrypted identification credentials from the portable memory device. Next, the user has his actual physical. . . the comparison is successful, the requested access is granted to the user. Otherwise, the requested access is denied by the **remote** access control site.

DETDESC:

DETD(4)

In . . . to be done in a fairly rapid manner. Lastly, and perhaps

most importantly, the credentials must be verifiable at a **remote** site or sites without access to a centralized data base.

DETDESC:

DETD(5)

The **remote** access control point verification equipment is a relatively low cost unit. This unit provides a high probability of authenticating proper. . .

DETDESC:

DETD(7)

Further, trusted computer 1 is connected via modems 25 to **remote** sites. These **remote** sites may input data to the trusted computer for generation of identification credentials or trusted computer 1 may transmit authorization information to **remote** sites. Trusted computer system 1 is further connected to encryption function 30. Information to be encrypted is sent from trusted. . .

DETDESC:

DETD(20)

As . . . memory medium, the encrypted CDS may also be sent from trusted computer 1, via modem 25 to one or more **remote** sites. The media writer function 40 would be provided at the **remote** sites, as well be described later.

DETDESC:

DETD(48)

If . . . from the requestor and digitizes this data. That is fingerprints, photographs, retinal scans or voice prints are taken at the **remote** validation site and digitized. Next, block 125 determines whether the biometric data collected from the requestor at the validation site. . .

CLAIMS:

CLMS(1)

We claim:

1. An unforgeable personal identification system for identifying users at **remote** access control sites, said unforgeable personal identification system comprising:
means for generating encrypted physically immutable identification credentials of a user;
said. . . according to a predefined one-way encryption algorithm to produce encrypted identification credentials;
portable memory means for storing said encrypted identification credentials;
said **remote** access control site including:
means for reading said encrypted identification credentials from said portable memory means;
means for directly inputting physically. . .

CLAIMS:

CLMS(12)

12. . . . claimed in claim 6, wherein there is further included:
modem means connected to said processor means and connected to said **remote** sites via a communication system, said modem means operating to transmit and to receive said encrypted data between said **remote** sites and said processor means; and
display means connected to said processor means, said display means operating to output said text. . .

CLAIMS:

CLMS(13)

13. An unforgeable personal identification system as claimed in claim 12, wherein said **remote** access control site further includes means for decrypting said encrypted identification credentials from said portable memory means, said means for. . .

CLAIMS:

CLMS(19)

19. An unforgeable personal identification system as claimed in claim 13, wherein said **remote** access control site further includes access control interface means connected to said means for comparing, said access control interface means. . .

CLAIMS:

CLMS(20)

20. An unforgeable personal identification system as claimed in claim 19, wherein said **remote** access control site further includes control processor means for controlling the operation of said **remote** access control site, said control processor means being connected to said means for reading, to said means for said inputting,. . .

CLAIMS:

CLMS(21)

21. An unforgeable personal identification system as claimed in claim 20, wherein said **remote** access control site further includes:
modem means connected to said control processor means and to said processor means via said communication system, said modem means operating to transmit said encrypted identification credentials between said **remote** access control site and said processor means;
keyboard means connected to said control processor means, said keyboard means for inputting data to said **remote** access control site;
display means connected to said means for decrypting, said display means operating to provide for observation of said physically immutable identification credentials of said user at said **remote** access control site; and
printer means connected to access control interface means for providing a hard copy record of said access.

CLAIMS:

CLMS(22)

22. A method for unforgeable personal identification having an authorization site and at least one **remote** access control site for allowing or denying access of a user, said method for unforgeable personal identification comprising the steps. . .
portable memory device including said encrypted identification credentials to said user;
said method for unforgeable personal identification further including at the **remote** access control site the steps of:
reading said encrypted identification credentials from said portable memory device of said user;
obtaining said. . .

CLAIMS:

CLMS(23)

23. A method for unforgeable personal identification as claimed in claim

22, wherein there is further included at the **remote** access site the step of decrypting said encrypted physically immutable identification credentials.

CLAIMS:

CLMS(25)

25. A method for unforgeable personal identification as claimed in claim 23, wherein there is further included at the **remote** access control site the step of denying said access to said user, if said comparison is unsuccessful.

CLAIMS:

CLMS(29)

29. A method for unforgeable personal identification as claimed in claim 28, wherein there is further included at said **remote** access control site the steps of:
determining whether said encrypted physically immutable identification credentials and data of said portable memory. . .

CLAIMS:

CLMS(30)

30. A method for unforgeable personal identification as claimed in claim 29, wherein there is further included at said **remote** access control site the step of utilizing said decrypted text information to support the access of said user.

CLAIMS:

CLMS(32)

32. A method for unforgeable personal identification as claimed in claim 31, wherein there is further included at said **remote** access control site the steps of:
reading said expiration data of said credentials;
determining whether said credentials are valid; and
rewriting said. . .
=